Magistrate Judge James P. Donohue

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. GVIDIV MATEESCU, a/k/a Mihai Podaru, and CLAUDIU TUDOR, Defendants.	CASE NO. MJ10-523 COMPLAINT for VIOLATION Title 18, United States Code, Section 1029(a)(4) and (b)(1)

BEFORE, the Honorable James P. Donohue, United States Magistrate Judge, U. S. Courthouse, Seattle, Washington.

The undersigned complainant being duly sworn states:

COUNT ONE
(Fraud in Connection with Access Devices)

On or about September 23, 2010, at Woodinville, within the Western District of Washington, GVIDIV MATEESCU and CLAUDIU TUDOR, knowingly and with intent to defraud produced, trafficked in, had custody and control of, and possessed device-making equipment, namely, an Automated Teller Machine (ATM) skimming device and a pin hole camera, which conduct affected interstate and foreign commerce, in that the aforementioned devices were installed on the ATM owned and operated by a federally insured financial institution, the scheme required use of the national banking channels, and the defendants

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

attempted to fraudulently obtain cash, funds, and monies belonging to and under the custody and control of said financial institution.

All in violation of Title 18, United States Code, Section 1029 (a)(4) and (b)(1).

And the complainant states that this Complaint is based on the following information:

I, MALCOLM FREDERICK, being duly sworn on oath, depose and say:

INTRODUCTION

1. I am a Special Agent with the United States Secret Service ("Secret Service") and have been so employed since March 31, 2008. I am currently assigned to the Seattle Field Office. I am a graduate of the Federal Law Enforcement Training Center located in Glynco, Georgia. I am also a graduate of the United States Secret Service Special Agent Training Program located in Beltsville, Maryland. Additionally, I am a graduate of the Washington State Basic Law Enforcement Training Academy. Prior to my employment with the Secret Service, I was a Commissioned Law Enforcement Officer with the Redmond Police Department for more than fourteen years. I also have a Bachelor of Arts Degree from the University of Washington. In the course of my official duties as a Special Agent with the Secret Service, I have been involved in cases involving credit card fraud, bank fraud, and counterfeit currency and securities.

2. As part of my training with the Secret Service, I have received specialized instruction on investigating financial crimes, including manufacturing and distribution of counterfeit currency, credit/debit card fraud, mail and wire fraud, access device fraud and identity theft. I have also received specialized training in the investigation of basic electronic crimes involving the use of computers and other electronic devices.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

3. This affidavit is made in support of a complaint for the arrest of Gvidiv MATEESCU and Claudiu TUDOR, for violations of Title 18, United States Code, Section 1029(a). The information contained in this affidavit is based on my own personal knowledge and information provided to me during my participation in this investigation, including information provided by other law enforcement officers and witnesses.

INVESTIGATION

4. Since June 2008, the U.S. Secret Service Electronic Crimes Task Force (ECTF), Seattle Field Office, has been conducting an ongoing investigation regarding credit/debit card skimming activity, which has targeted Automated Teller Machines (ATM) in Western Washington. The ECTF is an investigative task force that is comprised of local law enforcement officers and agents from the Secret Service.

A. Skimming and skimming devices

5. Credit/debit card "skimming" is the theft of credit/debit card information used in an otherwise legitimate transaction. Among other techniques, suspects often use manufactured plastic materials that look similar to parts of the face plate of an ATM machine. Once this plastic material is fabricated, an electronic card reader is placed inside the plastic. This small device ("skimmer" or "skimming device") will store the information, or track data, of an unsuspecting victim's bank card. Suspects can place the plastic device over the actual ATM card reader portal and intercept bank card information as the bank card passes through the device.

6. In conjunction with these skimming devices, suspects will routinely install small "pin hole" cameras above or to the side of the ATM key pad. These cameras capture a victim's Personal Identification Number (PIN) as the customer uses the ATM machine. The times on the skimming device are synchronized with the recorded times of the camera, which enables the

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

suspects to match a victim's PIN with the information taken from the bank card. Often times these cameras are installed using tape, glue, or other types of materials.

7. Skimmers are equipped to hold hundreds or potentially thousands of bank card numbers. Most skimmers have an integrated USB port, which allows data captured on the skimmer to be downloaded onto a laptop or desk top computer.

8. Suspects will typically retrieve their skimming devices from ATM machines, connect the skimming devices to a computer, and then download the victim bank account data. Typically, suspects will then transfer or "re code" victim bank account information onto blank credit/debit card stock, also known as white plastic. Suspects have also been known to re code stolen bank account data onto store gift cards.

9. Once this process is complete, suspects use the newly made cards to access victim bank account information at any available ATM machine. Typically, suspects will withdraw cash and also purchase consumer goods and merchandise within one month's period of time from the date that the debit card account was "skimmed."

10. All the equipment needed to conduct credit/debit card skimming as described above is available on the Internet. Moreover, based on my training and experience, an illegal skimming operation requires the use of a computer system to download the information from the skimmer and the pin hole camera and to manufacture counterfeit or fraudulent cards encoded with victim's account information.

B. Investigation into incidents of skimming activity

11. This investigation has revealed that Claudiu TUDOR and Gvidiv MATEESCU, and additional known and unknown suspects, have placed multiple electronic skimming devices as well as video surveillance devices, on various ATMs and ATM vestibule entrance doors

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

located at several different financial institutions and other locations in Western Washington.

12. The investigation has also determined that there are at least seven known federally insured financial institutions, including, but not limited to, Boeing Employees' Credit Union (BECU), that have recently had skimming devices and pin hole video cameras placed on their ATMs or ATM vestibules. Through my investigation and experience, I also know that BECU is a financial institution as defined by Title 18, United States Code, Section 20.

13. The investigation has revealed, among other things, that between September 9, 2010 and October 9, 2010, skimming devices have been placed on several BECU ATMs in the Seattle area, resulting in customer accounts being compromised. A review of this ATM surveillance video by BECU investigators and law enforcement revealed that two specific male individuals, Claudiu TUDOR and Gvidiv MATEESCU, can be identified at multiple BECU ATM locations, often on different days, actively participating in the placement of skimming devices. In several instances, TUDOR and MATEESCU are wearing the same clothing.

14. This investigation has also revealed that between, but not limited to, September 9, 2010 and October 9, 2010, on numerous occasions, various persons, known and unknown, have been captured on video surveillance using various BECU ATMs in the Seattle area to withdraw cash from customer accounts, without authorization or legal authority. The known resulting loss amount during this narrow time frame exceeds $328,906.00, and, I expect, will increase as the investigation continues. The two suspects discussed herein, TUDOR and MATEESCU, are among the persons observed engaging in such conduct.

15. One specific skimming incident occurred on September 19, 2010, at the BECU ATM located at 4250 NE 4th Street in Renton, Washington. The ATM surveillance video depicts two male suspects, TUDOR and MATEESCU, placing and later removing a skimming

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

device on the ATM between 3:24 p.m. and 4:16 p.m. Bellevue Police Detective Shelby Shearer was then able to positively identify one of the suspects as Claudiu TUDOR by comparing his Washington State driver's license photo to the ATM surveillance photographs. Additionally, Detective Shearer, with the assistance of Kirkland Police Detective Don Carroll, was able to positively identify the second individual as Gvidiv MATEESCU. MATEESCU had been previously identified by Detective Carroll as part of the investigation into ATM skimming activity.

16. Another specific skimming incident occurred on September 23, 2010, at the BECU ATM located at 13910 NE Mill Plaza in Woodinville, Washington. The ATM surveillance video, which was taken at approximately 3:20 p.m., captured images of Gvidiv MATEESCU approaching the ATM carrying a Wilson tennis racket case. MATEESCU removes a skimming device and video camera from the tennis racket case and places both devices on the BECU ATM. About twenty minutes after MATEESCU installs the skimming device, TUDOR is seen approaching this ATM. On this same date, at approximately 4:30 p.m., deputies with the King County Sheriff's Office responded to a citizen's complaint of two suspicious individuals loitering around this particular BECU ATM in Woodinville. Upon their arrival, the deputies contacted the two male subjects. One of these subjects identified himself to the deputies as Gvidiv MATEESCU. Deputies later discovered and removed a pin hole camera and a skimming device from this BECU ATM. I have reviewed surveillance images relating to this incident and recognize the two suspects as TUDOR and MATEESCU. Attached as Exhibit A are surveillance images from the September 23, 2010 incident in Woodinville.

17. Brian Orr, a Bellevue Police Department Evidence Technician, lifted a viable fingerprint from the underside of the pin hole camera device that had been mounted on the

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

BECU ATM in Woodinville. Carol Nicoll, the Bellevue Police Department Forensics Services Unit Manager, who has thirty-five years of forensic identification training and experience, compared this fingerprint to known fingerprints belonging to TUDOR. Nicoll positively identified the recovered fingerprint as belonging to TUDOR.

18. Additional elements and facts from this ongoing investigation have confirmed that TUDOR and MATEESCU are associates. I personally witnessed a police vehicle stop in Renton, Washington. During that stop MATEESCU was identified as the driver. A short time prior to this police stop, this same vehicle driven by MATEESCU had been observed leaving TUDOR's residence in Renton, Washington.

C. Arrest of MATEESCU and TUDOR

19. On November 6, 2010, a joint multi-agency surveillance operation, which included agents and officers from Bellevue Police Department, Seattle Police Department, King County Sheriffs Office, Kirkland Police Department, the U.S. Secret Service, and Immigration and Customs Enforcement, took place in King and Pierce Counties. One of the primary goals of this operation was to arrest known suspects who investigators from the above mentioned agencies had probable cause to arrest for either placing skimmers or attempting to use cloned bank cards for their personal benefit. The ongoing investigation had already identified Claudiu TUDOR and Gvidiv MATEESCU as known card skimmers.

20. During this operation, static surveillance was established at several previously identified locations of interest, including residences associated with TUDOR, who was, by this time, an individual known to engage in unlawful skimming activities.

21. At approximately 7:00 p.m., King County Sheriff's Office Sergeant Jon Mattsen and his surveillance team witnessed Claudiu TUDOR exit a known apartment residence and get

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

into a GMC SUV. A Washington State Department of Licensing records check revealed that the vehicle was a rental. Based on my training and experience, I know that rental vehicles are commonly used to commit crimes by skimming suspects so that their personal vehicles are not traced back to them. The surveillance team then followed him as he drove to an Extended Stay Motel in Renton. At the Extended Stay Motel, members of the surveillance team witnessed TUDOR pick up two male subjects.

22. The surveillance team then followed TUDOR and observed the men engage in suspicious activity at two different BECU ATM locations, in Puyallup and Maple Valley. For instance, at the former location, members of the surveillance team observed TUDOR place several cards into the BECU ATM machine. TUDOR and one of the other male subjects, believed to be Gvidiv MATEESCU, placed an unknown item into a nearby garbage can. TUDOR and the other man then walked around a nearby building and then came back to the ATM machine. TUDOR and the other man then retrieved the unknown item back out of the garbage can before walking away.

23. At approximately 11:00 p.m., Sergeant Mattsen advised that his surveillance team had stopped the GMC SUV as it was returning to the Extended Stay Motel in Renton. As the GMC SUV was arriving, the surveillance team took TUDOR and a second male subject, later identified as MATEESCU, into custody.

24. Upon arrest, MATEESCU presented detectives with a Romanian identification card and identified himself as Mihai Podaru, date of birth [redacted]1979. Detective Shearer drove to the scene and immediately recognized the male suspect as Gvidiv MATEESCU. This investigation has revealed that MATEESCU has a history of using aliases and false identification documents. MATEESCU also had several debit cards and a green "overlay" skimming device in

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

his possession. Detective Shearer identified this device as appearing identical to the device recovered from the BECU ATM machine in Woodinville, Washington, on September 23, 2010. MATEESCU also had in his possession $1,145.28 in cash, of which, $1,100.00 was in $100 dollar bills. Detective Shearer later confirmed that BECU ATMs dispense $100 bills.

25. Sergeant Mattsen asked TUDOR which room at the Extended Stay Motel he was staying in. TUDOR told Sergeant Mattsen that he could not remember the room number, but he would show him the room. TUDOR then led Sergeant Mattsen upstairs. TUDOR told Sergeant Mattsen again that he could not remember where the room actually was. As TUDOR led Sergeant Mattsen around, they walked by Room #106. As they walked by, TUDOR suddenly began yelling in a foreign language, believed to be Romanian. Sergeant Mattsen later stated that he did not realize it at the time, but TUDOR probably yelled something to someone inside Room #106.

26. Bellevue Police Detective Ray Lofink contacted the front desk manager of the Extended Stay Motel and was able to obtain a copy of the Motel registry. The registry showed TUDOR as renting Room #106.

27. Sergeant Mattsen walked around the outside of Room #106 to look at the unit. He then advised that the room had been breached and that the outside screen was off and the window was open. Mattsen advised officers on scene of the exigent circumstances that one or more people might be inside the room or that someone might have exited and that entry must be made for the preservation of evidence and officer safety. Detective Shearer assisted Sergeant Mattsen in entering the room to clear it of any persons or to ensure the non-destruction of evidence. Officers determined that no one was inside Room #106, but it appeared as though one or more

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

persons had fled through the window. Officers then backed out of the unit and secured it pending a search warrant application for the premises.

D. Items Seized

28. On November 7, 2010, Detective Shearer executed a search warrant issued by King County Superior Court Judge Richard McDermott on Room #106 at the Extended Stay Motel. Detectives with the Bellevue Police Department, Kirkland Police Department, and agents with the U.S. Secret Service assisted in executing this search warrant and located several items of evidence.

29. Items that are consistent with tools and supplies used to manufacture and install skimming devices and manufacture fictitious identification documents, glue, a razor knife, a cutting board, and a roll of plastic sheeting were located in the room. Also seized during the search were several electronic devices: two Toshiba laptop computers, one Dell laptop computer, four cellular phones, and two Virgin Mobile wireless USB devices. During the search both of the Toshiba laptop computers were found set up next to each other on a desk. Both computers were powered on. Additionally, one of the computers had a Virgin Mobile wireless device plugged into its USB port. An additional Virgin Mobile wireless USB device was found sitting on the desk next to the laptops. These type of USB devices are used as wireless connections to the internet.

30. Among the items found during the search, Detectives located a suitcase in the closet, which contained numerous fictitious identification documents: one Russian Visa, one Swedish passport, one Republic of Slovakia passport, one Oregon driver's license, one Republic of Slovakia driver's license, and one Swedish driver's license. MATEESCU's picture was on each of the identification documents that contained images, but there were three different names

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

used on these six different documents—none of which listed MATEESCU's name. During the search, Detectives also collected four cellular phones found in a suitcase located in the same closet where the fictitious identification documents were found.

31. Detective Shearer also executed a King County Superior Court search warrant on the GMC SUV that had been driven by TUDOR. During a search of this vehicle, Detectives located a genuine Romanian passport and a birth certificate in MATEESCU's name hidden in the vehicle's spare tire equipment compartment, as well as two additional cellular phones.

32. Based on my training and experience, I know that it is common for persons engaged in access device fraud, as well as aggravated identity theft and identification document fraud, and persons engaged in criminal conspiracies to commit such offenses, to use digital devices, including computers, USB devices, mobile or cellular telephones, blackberries, "smart phones," and electronic storage and communication devices, as tools or instrumentalities in committing criminal activity. Among other things, these devices are commonly used to capture, store, transfer, and transmit images, files, document "templates," graphic files, and data associated with victim's bank account information, such as the data obtained through use of the skimmers and the pin-hole cameras. These devices are also commonly used to manufacture fraudulent debit/credit cards using stolen data. Moreover, based on my training and experience, I know that persons engaged in schemes involving skimming devices often work in groups or operate in larger "rings," and in turn utilize pagers, mobile and cellular telephones, and other electronic devices to communicate with conspirators and others related to the scheme, to coordinate their actions, and otherwise to facilitate the scheme. I also know that, in the modern age, cellular phones and smart phones have many functions similar to computers and can, for example, be used to store, receive, and transmit enormous amounts data and information as well

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

as to access, send, and receive e-mail. For the reasons stated above, it is my belief that the items referenced above represent evidence, tools, and instrumentalities in the commission of the criminal activity described herein.

CONCLUSION

33. Based upon the information set forth above, I submit that there is probable cause to believe that the defendants, Gvidiv MATEESCU and Claudiu TUDOR, did knowingly and intentionally commit access device fraud, in violation of Title 18, United States Code, Section 1029, as alleged in Count One of this complaint, among other crimes.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and ability.

MALCOLM FREDERICK
Special Agent, United States Secret Service

Based on the Complaint and Affidavit sworn to before me, and subscribed in my presence, the Court hereby finds that there is probable cause to believe the Defendants committed the offense set forth in the Complaint.

Dated this 13th day of December, 2010.

Hon. James P. Donohue
United States Magistrate Judge

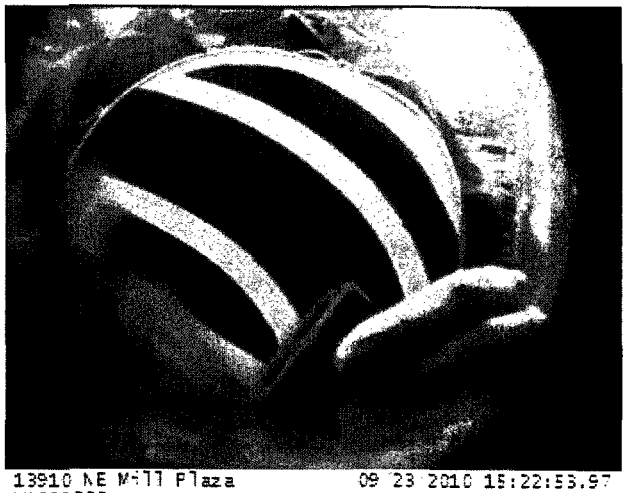
UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Exhibit A

Timeline of activity:

September 23rd 2010 15:20hrs the overhead camera was installed.

September 23rd 2010 15:21hrs the magnetic skimming device was installed.



September 23rd 2010 15:47hrs known individual involved in skimming walks up to atm but does not use machine